Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended)

Claim 2 (previously amended)

Claim 3 (currently amended)

Claim 4 (currently amended)

Claim 5 (previously amended)

Claim 6 (currently amended)

Claim 7 (previously amended)

Claim 8 (previously amended)

Claim 9 (previously amended)

Claim 10 (currently amended)

Claim 11 (previously amended)

Claim 12 (original)

Claim 13 (previously amended)

Claim 14 (previously amended)

Claim 15 (currently amended)

Claim 16 (cancel)

Claim 17 (previously amended)

claim 18 (previously amended)

Claim 19 (currently amended)

Claim 20 (previously amended)

Claim 21 (previously amended)

Claim 22 (currently amended)

Claim 23 (previously amended)

Claim 24 (currently amended)

Claim 25 (previously amended)

1. (Currently amended)

A method of creating certificates with redundant information to certify several keys, wherein each of the certificates comprises a defined number of data elements which at least contain information on a certification body (issuer of the certificate), a user of the certificate and a key certified by the certificate, ~~characterized by~~ comprising the following steps:

~~a) specification of a request for certification of one or more of several keys by the certification body for the user;~~

[[b)]] a) ~~if in step a) only one key is to be initially certified, and no basic certificate is yet available for the user,~~ creation by the certification body of a basic certificate for the user ~~with a~~ containing a single recitaiton of a defined number of data elements therein which elements are identical or redundant for the several keys of the user in conjunction with the certification body;

[[c)]] b) addition of an identifying characteristic to the basic certificate;

[[d)]] c) generation of a digital signature for the basic certificate;

[[e)]] d) addition of the digital signature to the basic certificate;

[[f)]] e) generation of a key pair;

[[g)]] f) creation of a supplementary certificate for the basic certificate which does not recite the redundant data elements but does contain [[with]] a key as set out in step [[f]] e), the identifying characteristic as set out in step [[c]] b) and additional data fields not registered by the basic certificate;

[[h)]] g) generation of a digital signature for the supplementary certificate;

[[i)]] h) addition of the digital signature to the supplementary certificate; and

~~j) use of an existing basic certificate for the only one key when~~ the ~~one key shares the redundant information with the existing basic certificates; and~~

[[k)]] i) use of the basic certificate created in step [[b]] a) for ~~future~~ other of the several keys in additional supplementary certificates that share with the supplementary certificate of step f) the redundant information [[with]] recited the basic certificate but like the supplementary certificate of step f) do not recite the redundant data elements.

2. (Previously amended)

The method in accordance with Claim 1, characterized in that the basic certificate comprises the following data elements:

- name of the certification body,
- user ID of the certification body,
- name of the user,
- user ID of the user, and
- identifying characteristic of the basic certificate.

3. (Currently amended)

The method in accordance with Claim [[1]] 2, characterized in that the supplementary certificates ~~comprises~~ comprise the following data elements:

- a signature algorithm,
- a key,
- serial number of the key,
- a validity period of the certificate,
- extensions, and
- an identifying characteristic of the basic certificate.

4. (Currently amended)

The method in accordance with Claim 1, where more than one key with the same validity period [[is]] are to be certified at one time~~, instead of steps b) - i) the following steps are executed~~ in step f), including the following steps:

aa) generation of several key pairs one for each of the keys ;

bb) generation of the basic certificate of step a) as a single group certificate (group certificate) for all the several keys with all data elements necessary for the individual keys and keys generated in step aa), with only a single recitation of data elements redundant to all the several keys in the group certificate;

cc) generation of a digital signature for the group certificate; and

dd) addition of the digital signature to the group certificate.

5. (Previously amended)

The method in accordance with Claim 4, characterized in that the basic certificate contains the following data elements:

- name of the certification body,
- user ID of the certification body,
- name of the user,
- user ID of user,
- type/version of the certificate,
- number and types of keys,
- a key,
- validity,
- serial number, and
- extensions.

6. (Currently amended)

The method in accordance with Claim 1 ~~characterized in that, if only~~ where one key is to be certified in step [[a]] i) and [[a]] the basic certificate of step a) already exists, ~~as stated in step j) or k), instead of steps b) - i)~~ including the following steps ~~are executed~~:

aa) definition of the basic certificate and reading of the identifying characteristics of the basic certificate ;

bb) generation of a key pair ;

cc) creation of a supplementary certificate for the basic certificate with additional data fields not registered by the basic certificate, wherein one of the keys is inserted into the supplementary certificate in step bb);

dd) insertion of the identifying characteristics in accordance with step aa) into the supplementary certificate to locate the associated basic certificate ;

ee) generation of a digital signature for the supplementary certificate; and

ff) addition of the digital signature to the supplementary certificate.

7. (Previously amended)

The method in accordance with Claim 6, characterized in that any supplementary certificates each contain the following data elements:

- a signature algorithm,
- a key,
- serial number of the key,
- validity period of the certificate,
- extensions, and
- identifying characteristic of the basic certificate.

8. (Previously amended)

The method for creating a certificate for simultaneous certification of several keys with the same validity period, wherein the certificate comprises a defined number of data elements which at least contain information on the certification body (issuer of the certificate), the user of the certificate and the key certified by the certificate, characterized by the following steps:

aa) generation of several key pairs;

bb) generation of a single joint or group certificate (group certificate) for several keys with all data elements necessary for the individual keys and keys generated in step aa), with the group certificate containing only a single recitation of data elements;

cc) generation of a digital signature for the group certificate; and

dd) addition of the digital signature to the group certificate.

9. (Previously amended)

The method in accordance with Claim 8, characterized in that the group certificate contains the following data elements:

- name of the certification body,
- user ID of the certification body,
- name of the user,
- user ID of the user,
- type/version of the group certificate,
- number and types of keys,
- key,
- validity,
- serial number, and
- extensions.

10. (Currently amended)

A method for creating a certificate for certification of a new key for a user, wherein the certificate comprises a defined number of data elements which at least contain information on a certification body (issuer of the certificate), a user of the certificate and the key certified by the certificate, wherein a basic certificate for the user already exists and the basic certificate comprises data elements which, in the certification process, are identical for the respective user in conjunction with the respective certification body, characterized by the following steps:

aa) definition of the basic certificate for the user and reading of the identifying characteristics of the basic certificate;

bb) generation of a key pair for the new key;

cc) creation of a supplementary certificate for the basic certificate with additional data fields not registered by the basic certificate, wherein one of the keys of the key pair generated in step bb) is inserted into the supplementary certificate ;

dd) insertion of the identifying characteristics in accordance with step aa) into the supplementary certificate to locate the associated basic certificate;

ee) generation of a digital signature for the supplementary certificate; and

ff) addition of the digital signature to the supplementary certificate.

11. (Previously amended)

The method in accordance with Claim 10, characterized in that the supplementary certificate contains the following data elements:

- a signature algorithm,
- a key,
- serial number of the key,
- validity period of the certificate,
- extensions,
- an identifying characteristic of the basic certificate.

12. (Original)

The method in accordance with Claim 8, characterized in that the key is a public key.

13. (Previously amended)

The method in accordance with Claim 1, characterized in that the basic certificate and the supplementary certificate are stored in a non-volatile memory of a chipcard.

14. (Previously Amended)

The method in accordance with Claim 4, characterized in that the basic certificate (group certificate) is stored in a non- volatile memory of a chipcard.

15. (Currently amended)

The method for ~~reading certificates created in accordance with Claim 1, characterized by the following steps~~ determining if a chipcard contains a relevant key to sign a message in the chip cards nonvolatile storage medium:

a) check of the nonvolatile storage medium for presence of basic certificates;

b) if a basic certificate is present, identification of ~~the necessary~~ a supplementary certificate with a suitable signature key ;

c) reading-in of the supplementary certificate into the chapcard RAM ~~of a system;~~

d) definition of the identification number of the basic certificate from the supplementary certificate; ~~and~~

e) reading-in of the basic certificate into the RAM.

f) when no basic certificate is identified checking of the storage medium for presence of group certificates; and

g) reading-in of a necessary group certificate into the RAM.

16. (Cancel)

17. (Previously amended)

The method for reading of certificates created in accordance with Claim 10, characterized by the following steps:

a) check of the storage medium for presence of group certificates; and

b) reading-in of a necessary group certificate into the RAM.

18. (Previously amended)

The method in accordance with Claim 17, characterized in that the storage medium is a non-volatile memory of a chipcard.

19. (Currently amended)

A computer program product on a computer usable medium for creating certificates to certify several keys sharing redundant information, wherein a certificate comprises a defined number of data elements which at least contain information on the certification body (issuer to the certificate), the user of the certificate and the key certified by the certificate, said computer program product comprising:

a) software code for specification of a request for certification of ~~at least~~ one of the several keys by a certification body for a user;

b) software code for creation of a basic certificate for the user with a defined number of data elements which, in the certification process, are identical for the respective user in conjunction with the respective certification body when initially only one key is to be certified, and no basic certificate is yet available for the user;

c) software code for the addition of an identifying characteristic to the basic certificate;

d) software code for the generation of a digital signature for the basic certificate;

e) software code for the addition of the digital signature to the basic certificate;

f) software code for generation of a key pair;

g) software code for creation of a supplementary certificate for the basic certificate with a key as set out in f), the identifying characteristic as set out in c) and additional data fields not registered by the basic certificate;

h) software code for generation of a digital signature for the supplementary certificate;

i) software code for addition of the digital signature to the supplementary certificate; and

j) software code for use of the basic certificate created in step b) with a future key[[s]] that shares the redundant information with the basic certificate by issuing an additional supplementary certificate with a new key pair.

20. (Previously amended)

The computer program product in accordance with Claim 19, characterized in that the basic certificate comprises the following data elements:

- name of the certification body,
- user ID of the certification body,
- name of the user,
- user ID of the user,and
- identifying characteristic of the basic certificate.

21. (Previously amended)

The computer program product in accordance with Claim 19, characterized in that the supplementary certificates comprise the following data elements:

- a signature algorithm,
- a key,
- a serial number of the key,
- a validity period of the certificate,
- extensions, and
- identifying characteristic of the basic certificate.

22. (Currently amended)

The computer program product in accordance with Claim 19, ~~characterized in that if~~ more than one key with the same validity period is to be certified at one time, including the following software code:

aa) software code for generation of several key pairs;

bb) software code for generation of [[a]] the basic certificate of step b) as a single certificate (group certificate) for several keys with all data elements necessary for the individual keys and keys generated in step aa), omitting the redundant data elements for the several keys by having only a single recitation of the redundent data elements in the group certificate;

cc) software code for generation of a digital signature for the certificate; and

dd) software code for addition of the digital signature to the certificate.

23. (Previously amended)

The computer program product software in accordance with Claim 22, characterized in that the group certificate contains the following data elements:

- name of the certification body,
- user ID of the certification body,
- name of the user,
- user ID of the user,
- type/version of the certificate,
- number and types of keys,
- a key,
- validity,
- serial Number, and
- extensions.

24. (Currently amended)

The computer program product in accordance with Claim 19, where a key is to be certified and [[a]] the basic certificate already exists, including the following software code:

aa) software code definition of the basic certificate and reading of the identifying characteristics of the basic certificate;

bb) software code for generation of a key pair;

cc) software code for creation of a supplementary certificate for the basic certificate with additional data fields not registered by the basic certificate, wherein one of the keys is inserted into the supplementary certificate by step bb);

dd) software code for insertion of the identifying characteristics in accordance with step aa) into the supplementary certificate to locate the associated basic certificate;

ee) software code for generation of a digital signature for the supplementary certificate; and

ff) software code for addition of the digital signature to the supplementary certificate.

25. (Previously amended)

The computer program product in accordance with Claim 24, characterized in that the supplementary certificate contains the following data elements:

- a signature algorithm,
- a key,
- serial number of the key,
- validity period of the supplementary certificate,
- extensions, and
- identifying characteristic of the basic certificate.